UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/749,057	12/30/2003	Daryl Carvis Cromer	RPS920030222US1	7390

61755 7590 11/30/2007

Kunzler & McKenzie
8 EAST BROADWAY, SUITE 600
SALT LAKE CITY, UT 84111

EXAMINER	
HENEGHAN, MATTHEW E	
ART UNIT	PAPER NUMBER
2134	

MAIL DATE	DELIVERY MODE
11/30/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/749,057	CROMER ET AL.	
	Examiner	Art Unit	
	Matthew Heneghan	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 September 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3-7 and 9-30* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3-7 and 9-30* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *30 December 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. In response to the previous office action, Applicant has amended claims 1, 3, 4, and 9-30 and cancelled claims 2 and 8.Claims 1, 3-7, and 9-30 have been examined.

2. All previous rejections under 35 U.S.C. 101 and 35 U.S.C. 112 and all previous objections have been withdrawn.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 1, 3, 9-14, 17-24, and 27-29 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent No. 7,058,807 to Grawrock et al.

As per claims 1, 19, 20, 22, 27, and 29, Grawrock discloses an embedded security system (a token) having PCRs (which are trusted, see column 6, lines 46-47) record integrity metrics (measurement values of trusted configurations) of processors

(which may be internal) and chipsets that are extended to the PCRs and seal cryptographic keys related to platforms (see column 5, lines 46-61). The chipsets may be devices physically connected to the computer system such as a disk drive (a data repository) (see column 4, lines 44-48). Encryption operations in sealing and unsealing the keys relating to a data center (i.e. encryption and decryption) are performed using the cryptographic keys that are based at least in part on the PCR digest values (see column 7, lines 1-19).

As per claims 9, 10, 12, and 17, the process is embodied in computer readable media (see column 6, lines 12-34).

As per claim 3, implementation is performed according to the TCG specification (see column 6, lines 10-16).

As per claims 11 and 21, the measurement is performed using a hash of the code (if it has firmware, then it is firmware code) (see column 5, lines 57-60).

As per claims 13, 14, 23, and 24, the unsealing of a key is done by the TPM by comparing the metric in the PCR to the current value (see column 10, lines 41-67).

Regarding claims 18 and 28, the TPM must be accessible without the sealed key, since it must be used to retrieve that sealed key.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 4-8, 15, 16, 25, 26, and 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 7,058,807 to Grawrock et al. as applied to claim 9 et al. above, and further in view of U.S. Patent Application Publication No. 2005/0021968 to Zimmer et al.

Regarding claim 4 and 5, Grawrock does not disclose the test being performed before the operating system loads.

Zimmer discloses testing pre-boot so that the TPM functionality may be authenticated before system operation (see paragraph 17).

Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Grawrock by testing pre-boot, as disclosed by Zimmer, so that the TPM functionality may be authenticated before system operation.

Regarding claims 6, 7, 15, and 25, Grawrock discloses the use of disk drives, but not removable media per se.

Zimmer discloses that removable media and firmware (non-volatile) may be used for the platform device (see paragraph 13). One skilled in the art would recognize that using removable media affords greater security by allowing for storage of the security information apart from the computer.

Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to use a removable disk for the platform device, as disclosed by Zimmer, to afford greater security by allowing for storage of the security information apart from the computer.

Regarding claims 16 and 26, Grawrock does not disclose the use of serial numbers in the platform configuration.

Zimmer discloses the usage of serial numbers in platforms to identify the correct platforms for using firmware updates (see paragraph 47).

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Grawrock by storing serial numbers on platforms, as disclosed by Zimmer, so that they can be used to identify the correct platforms for using firmware updates.

Response to Arguments

5. Applicant's arguments filed 26 September 2007 regarding the rejections under 35 U.S.C. 102 and 35 U.S.C. 103 have been fully considered but they are not persuasive.

The cryptographic key in Grawrock is sealed by combining it with a digest value; they are combined using the permanent public key (see column 7, lines 4-9). This teaches to the claims as recited. A second level of encryption is not required by the claims.

Regarding the combining of Grawrock and Zimmer, an implementation of the invention of Grawrock using Zimmer's teachings would yield the claimed invention. The reading and usage of a sealed key is necessary for Zimmer's pre-boot process as it is applied to Grawrock's invention. Regarding the use of removable media, Zimmer introduces the use of removable media, and the case has been made above why one skilled in the art would use those media in the manner of Applicant's claimed invention.

Conclusion

6. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew E. Heneghan, whose telephone number is (571) 272-3834. The examiner can normally be reached on Monday-Friday from 8:30 AM - 4:30 PM Eastern Time.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand, can be reached at (571) 272-3811.

Any response to this action should be mailed to:
Commissioner of Patents and Trademarks
P.O. Box 1450
Alexandria, VA 22313-1450
Or faxed to:
(571) 273-3800

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571) 272-2100.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Matthew Heneghan/

Primary Patent Examiner, USPTO AU 2134

November 28, 2007